Streetsbrook Infant & Nursery School

E-safety Policy, including Acceptable Use

STREETSBROOK INFANT & NURSERY SCHOOL

'Learning for Life'

At Streetsbrook, we strive to provide an equal chance for all to become responsible citizens who lead happy and fulfilled lives, and are equipped with the skills and abilities to shape the world they live in.

Our values are:

Desire to Learn

To enjoy the lifelong process and challenge of learning; alone and with others

Love and Respect

To have respect for ourselves, others and the environment, recognising and celebrating individual lifestyles, cultures and faiths

Happiness

Developing successful relationships where individuals can build and follow their dreams

Confidence

Having the self-belief to embrace and follow your own choices.

Being a Good Citizen

Making a positive contribution to communities on a local and global scale

Contents

Introduction

Using the Internet is now an everyday occurrence for most adults and children. There are numerous ways in which children can access the Internet, including:

- websites
- learning Platforms and Virtual Learning Environments
- email and Instant Messaging
- chat rooms and social networking
- blogs and wikis
- podcasting
- video broadcasting
- music and video downloading / streaming
- gaming
- mobile / smart phones and tablet computers with text, video and/or web functionality

However, the increased use of technology at school and home also exposes children to a number of risks and dangers. In its simplest form E-safety is about ensuring children use new technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

As with most things, awareness and education are central to safe Internet usage. This policy outlines how the principle of E-safety will be managed at Streetsbrook Infant and Nursery School.

Why Internet use is important

The Internet is an essential element in the 21st century life for education, business and social interaction and its use is part of the statutory curriculum, a necessary tool for learning. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Therefore the school has a duty to provide teachers and children with quality Internet access as part of their teaching and learning experiences.

As many of our children use the Internet widely outside school they will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of the Internet to Education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries and to experts in many fields for children and staff

- inclusion in the National Education Network connecting all UK schools

- educational and cultural exchanges between children world-wide

- vocational, social and leisure use in libraries, clubs and at home

- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with SMBC and DCFS
- access to learning wherever and whenever convenient

How the Internet enhances learning

Internet access will be planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of children. Staff guide children in on-line activities that will support the learning outcomes planned for the children' age, maturity and ability. The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of children provided by the LA.

As part of the school's Computing Scheme of Work for KS1, children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Children will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.

Children

An E-safety training programme will be delivered to all children to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools. When working online children will be taught to be S.M.A.R.T:

Safe ~ to remain safe by protecting personal information

Meeting ~ never meet somebody you have only been in touch with online without a parent or guardian

Accepting ~ do not accept email, files or messages from people you don't know

Reliable ~ not all information on the Internet is true, including the identity of others

Tell ~ it is never too late to tell a parent, carer or responsible adult if someone or something makes you feel afraid online

Children will be informed that Internet use will be monitored and rules for Internet access will be posted in all networked rooms.

E-Safety is embedded as part of the Computing curriculum and is an integral part of our Computing sessions.

Staff

The school's E-safety Policy will only be effective if all staff subscribe to its values and methods. Therefore, teaching students and cover or supply staff should not be asked to take charge of an Internet activity without full and proper preparation with a member of the school's teaching staff.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using the Internet for both professional and personal use both on and off the school premises. All staff will be given the School E-safety Policy and its importance explained. A copy will be held on the schools network in the policies folder on the 'teachers' drive and published on the school's Website.

Staff development in safe and responsible Internet use and on the school E-safety Policy will be provided as required.

Staff must not knowingly access or download pornographic, offensive, defamatory or other illegal material available on the Internet This will be treated as a serious disciplinary offence, and may lead to dismissal.

Parents

Parents' attention will be drawn to the School E-safety Policy at curriculum meetings, in newsletters, the school brochure and on the school website.

A partnership approach with parents will be encouraged through:

- Consultation with the Parent Partnership Team;
- a letter will be sent out to parents at the beginning of each academic year to make them more aware of E-safety
- Parents seeking additional information to safeguard their children when using the Internet will be referred to organisations listed on the school's website.

Any Internet issues that arise in school will be handled sensitively to inform parents without alarm.

Internet Access

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SMBC can accept liability for the material

accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.

Parents will be informed that children will be provided with supervised Internet access. Most children when using the Internet will be directly supervised whilst accessing specific, approved on-line materials. However to meet the needs of our more able children and encourage independent learning some children, following appropriate teaching, will have access to the Internet for independent research.

The school will maintain a current record of all staff and children who are granted Internet access, all of whom must read, sign and abide by the 'Acceptable ICT Use Policy', see Appendix (i) before using any school ICT resource (parents will be asked to sign and return a consent form for pupil access.) The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Evaluation of Internet content

Children need to understand how to extract, interpret and use information and evaluate its significance. Respect for copyright and intellectual property rights should also be taught. The school will ensure that the copying and subsequent use of Internet derived materials by staff and children comply with copyright law.

Children and staff may occasionally be confronted with inappropriate material, despite filtering. If staff or children discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services, and where appropriate the school E-safety officer.

Managing published content

The schools website is used to celebrate children' work, promote the school and publish resources for projects or homework.

The schools website must comply with the school's guidelines for publications including respect for intellectual property rights and copyright. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. All materials for publication on the school's web pages must be, prior to publication, reviewed and authorised by the headteacher.

The contact details on the website should only include the school address, email and telephone number. Staff or children's personal information will not be published, to avoid spam harvesting.

Publishing images of staff and children

Photographs that include children and/or staff add a liveliness and interest to a website. Nevertheless the security of staff and children must come first.

Children's full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of

children are published on the school website and the teaching staff will check any children present in a photograph for publication on the school's web pages has parental consent before publication.

Managing social networking

Social networking sites and newsgroups will be blocked unless a specific use is approved.

Children are taught never to give out personal details of any kind which may identify them or their location, for example their full name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc, when using the Internet.

Children are advised not to place personal photos on any social network space. They should also consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph that could identify the student or his/her location, for example a house number, street name, school or shopping centre. Children should be advised on security and encouraged to set passwords and deny access to unknown individuals and unwanted communications. Children are encouraged to invite known friends only and deny access to others. They will also be advised not to publish specific and detailed private thoughts.

Teachers' official blogs or wikis should be password protected and only run from the school website or the SMBC extranet. Teachers should not run social network spaces for students on a personal basis or communicate with children through private social networking sites, even on educational matters, but should use official sites sanctioned by the school.

When using social networking sites for personal use teachers must maintain school confidentiality and not publish school specific information. Additionally staff should not grant children or parents, except where a relationship existed previously, access to their published material.

The school is aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments. Incidents of bullying through social networking will be dealt with in line with the school policy behaviour, which includes bullying.

Managing filtering

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school currently works in partnership with Solihull MBC to ensure filtering systems are as effective as possible. Solihull MBC uses a blocking strategy to prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day and therefore, if staff or children discover unsuitable sites, the URL, time and date must be reported to the school E-safety coordinator without delay.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Managing Email

Email use can bring significant educational benefits and interesting projects between neighbouring schools or even continents can be created. However, un-regulated email can provide routes to children that bypass the traditional school boundaries and spam, phishing and virus attachment make email an important E-safety issue.

As with social networking, email can be used to bully others. Incidents of bullying through email will be dealt with in line with the school policy on behaviour, which includes bullying.

The following rules and guidelines for the use of the school's email system should always be followed:

- children may only use approved email accounts on the school system;
- children must immediately tell a teacher if they receive offensive email;
- children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission;
- use of words included in the filtering/checking 'banned' list will be detected and logged by SMBC EICT Services;
- excessive social email use can interfere with learning and may be restricted;
- email sent to external organisations by children should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- the forwarding of chain letters is not permitted;
- email addresses should be published carefully, to avoid spam harvesting
- staff must use their school email for school-related work

Video Conferencing and VoIP (Internet Telephony)

Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. It is essential to establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class. In the event that the school acquires video conferencing or VoIP hardware the following guidelines should be considered.

All video conferencing equipment in the school must be switched off when not in use and not set to auto answer. IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Use over the non-educational network cannot be monitored or controlled. Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.

External IP addresses should not be made available to other sites and video conferencing contact information should not be put on the school website.

School video conferencing equipment should not be taken off school premises without permission. The equipment must be secure and if necessary locked away when not in use. Responsibility for the use of the video conferencing equipment outside school time needs to be established with care. Only key administrators should be given access to the video conferencing system web or other remote control page available on larger systems. Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.

Children should ask permission from the supervising teacher before making or answering a videoconference call. All video conferencing must be supervised by the class teacher and must be authorised by parents and guardians before their children to take part in videoconferences.

When recording a lesson, written permission must be obtained from all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material must be stored securely and if third-party materials are to be included, these must be checked to avoid infringing the owners' Intellectual Property Rights (IPR).

Emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. These emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones are not be used for personal use during lessons or formal school time. (Please see the Safeguarding / Child Protection policies for further details). Tablet computers are licensed to be used by Early Years and Childcare staff as part of assessment and are not currently used by children in school.

When working with children off site staff will be issued with the school's mobile telephone. This is for the use of the supervising member of staff only.

Managing information services

The security of the school information systems will be reviewed regularly and antivirus protection will be updated regularly. All security strategies will follow Solihull MBC guidelines.

The ICT technician regularly reviews system capacity and files held on the school's network are regularly checked. Unapproved system utilities and executable files will not be allowed in children' work areas or attached to emails.

Portable media may not be used without specific permission followed by a virus check. The school will supply each member of staff with a password protected flash drive. However, children's personal information should not be stored on any portable media.

Protecting personal data

Personal data will be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual).

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

E-safety complaints

Parents and children will need to work in partnership with staff to resolve issues of E-safety as they arise. E-safety complaints will be dealt with using the normal complaints processes for the school. Potential child protection or illegal issues, however, must be referred to the school Designated Member of Staff for Child Protection, Mrs Louise Minter. A senior member of staff will deal with formal complaints of Internet misuse and any complaint about staff misuse of the Internet must be referred to the Headteacher who should use the agreed SMBC procedures.

Community use of ICT and the Internet

Where appropriate the school will liase with local organisations to establish a common approach to E-safety. The school will be sensitive to Internet related issues experienced by children out of school, e.g. social networking sites, and offer appropriate advice. The Internet is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. Ideally, young people would encounter a consistent policy to Internet use wherever they are.

In community Internet access there is a fine balance to be achieved in ensuring 'freedom of information' whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation is developing access appropriate to its own client groups and children may find variations in the rules and even unrestricted Internet access. Although policies and practices may differ, community partners adhere to the same laws as schools with respect to content, copyright and misuse. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with children on the reasons for the differences would be worthwhile. Children need to know how to stay safe online wherever they are.

Sensitive handling of cultural aspects is important. For instance filtering software may need to work across community languages and school Internet policies may need to reflect the children' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

Policy Review

The E-safety policy has been written by the school, building on the 'SMBC Schools E-safety Policy' and government guidance. It has been agreed by the senior management and approved by Governors, the Parent Partnership Team and the School Council.

The E-safety Policy and its implementation will be reviewed regularly by the school's appointed E-safety Coordinator (the Designated Member of Staff for Child Protection). This review will be carried out in consultation with the Health & Safety Manager, ICT Subject Leader, IT Technician and other relevant staff.

The Headteacher will ensure that the E-safety Policy is implemented and compliance with the policy monitored.

This policy will be reviewed in Spring 2016

E Fogarty

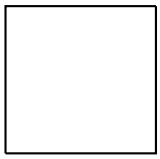
February 2015

This policy was ratified by the Governing Body in June 2015.

Signed: ……. Chair of Governors

Signed: ……..Headteacher

Appendix (i)



Streetsbrook Infant School and Nursery
Acceptable Use Policy for Children

This Acceptable Use Policy is intended to ensure that:

- our children will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

At Streetsbrook we ensure that our children have good access to ICT to enhance their learning and we, in return, expect the children to agree to be responsible users.

Acceptable Use Policy Agreement (Key Stage 1):

I want to feel safe all the time.

When using the Internet, I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are okay
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not load photographs of myself on to the computer without my teacher knowing
- never agree to meet a stranger

I know that anything I do on the computer may be seen by someone else.

Name of Child:…… Class:……..

Signed:…… Date:……..

Streetsbrook Infant School and Nursery
Acceptable Use Policy for Staff

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of ICT in their everyday work

The school will ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

Acceptable Use Policy Agreement:

I agree that I will:

- only use personal data securely
- implement the schools policy on the use of technology and digital literacy
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- only give access to appropriate users when working with blogs or wikis etc
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the E- Safety Leader, Elliot Fogarty
- ensure that videoconferencing is supervised appropriately for the learner's age
- read and sign the acceptable use policy
- pass on any examples of Internet misuse to a senior member of staff
- post any supplied E-Safety guidance appropriately

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (including child pornography)
    - promoting discrimination of any kind
    - promoting racial or religious hatred
    - promoting illegal acts
    - breach any Local Authority/School policies, e.g. gambling
    - do anything which exposes children in my care to danger
    - any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Name of Staff Member ……..

Signed ……. Date…….

Streetsbrook Infant School and Nursery

Acceptable Use Policy for Schools and Governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed every two years
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Name of Governor…….

Signed ……. Date…….

Appendix (ii)

SOLIHULL MBC HEALTH & SAFETY RISK ASSESSMENT

ACTIVITY / AREA COVERED BY THIS ASSESSMENT: E-Safety

DIRECTORATE / DIVISION / SECTION: Streetsbrook Infant and Nursery School
Whole School

Impact/severity				
	High	6	7	9
	Med	3	5	8
	Low	1	2	4
		Low	Med	High
		Likelihood		

Hazard	Persons at Risk	Risk Description	Gross / Initial risk		Risk Level	Current Mitigating Action (Existing Controls /Precautions)	Net risk		Risk Level	Owner
			Likelihood	Impact / Severity			Likelihood	Impact/ Severity		
Child reveals private password	All	Child reveals their password (for either logging on or for email) to a friend	High	Low	4	Class teacher to remind children about the importance for keeping passwords private.	High	Low	4	
An image , text or video has been viewed that makes the child feel scared, anxious or uncomfortable, including adverts	All	When on the Internet, a child views an image, text or video that makes them feel uncomfortable. This can include clicking or viewing ad advert that is on a certified website	Low	High	6	The school internet access is designed for educational use and will include appropriate filtering and monitoring. Teachers monitor which websites the children are visiting to see whether there is the potential for this hazard to occur.	Low	High	6	
An email has been received off an unknown sender	All	Whilst accessing email, a child has received an email off an unknown sender	Low	High	6	Children's school emails should only receive emails from members of staff or fellow children. The child's email address should only be	Low	High	6	

						accessed and made available to those within the school setting.				
Personal information (phone numbers, addresses) have been shared to unknown receivers		A child shares personal information to another Internet user	Low	High	6	Available websites at school do not provide opportunities for children to share information with strangers. Children's email should only receive emails off staff or other children. Children to be taught of the importance to keep personal information private between each other.	Low	High	6	
A nasty message\ email has been received	All	A child opens an email that contains a nasty or abusive email.	Low	High	6	Children's email should only receive emails off staff or other children. Should the nasty message be off a child in the same school, teacher to deal with the sender of the message in line with the school behaviour policy and logged in class concern book. To be followed up via Child Protection DMS if necessary.	Low	High	6	
Video message received from an unknown source	All	Whilst connected via video messaging, a request for a video message is received from an unknown source	Low	High	6	Video messaging to run through Solgrid connect which ensures peer to peer safety	Low	High	6	
A virus or spyware has been downloaded	All	Whilst opening an email or viewing a webpage, a virus or spyware has been unintentionally downloaded	Low	High	6	Solgrid checks for viruses in the attachments of incoming and outgoing external email. Websites that provide risk of viruses or spyware are filtered by Sophos.	Low	High	6	

A child states of something they have accessed at home that is not age appropriate	All	A child discloses to an adult (or an adult overheard a child telling their friend) that they have viewed something at home that is not appropriate for their age.	Medium	Medium	5	Depending on the severity, teacher to log in class concern book and action to be followed up via Child Protection DMS if needed.	Medium	Medium	5	

ASSESSED BY (PRINT)	E. Fogarty	SIGNED E. Fogarty	DATE ASSESSED 15.02.15	
MANAGER (PRINT)	SIGNED [signature]	DATE 15.2.15		